SMART CARDS

Kuldeep Yadav,Kunal Taneja,Megha Chauhan
Student, Department of ECE, Dronacharya College of Engineering, Gurgaon, India

***Abstract*- The term *smart card* has been used to describe a class of credit card–sized devices with varying capabilities: stored-value cards, contactless cards, and integrated circuit cards (ICCs). All of these cards differ in functionality from one another and from the more familiar magnetic stripe cards that standard credit, debit, and ATM cards use. It's the ICC that's of most interest to the computer industry because it's able to perform more sophisticated operations, including signing and key exchange.**

I. INTRODUCTION

The need for security and enhanced privacy is increasing as electronic forms of identification replace face-to-face and paper-based ones. The emergence of the global Internet and the expansion of the corporate network to include access by customers and suppliers from outside the firewall have accelerated the demand for solutions based on public key cryptography technology. A few examples of the kinds of services that public key cryptography technology enables are secure channel communications over a public network, digital signatures to ensure image integrity and confidentiality, authentication of a client to a server (and vice versa), and the use of smart cards for strong authentication. The Microsoft Windows operating system platform is smart card–enabled and is the best and most cost-effective computing platform for developing and deploying smart card solutions.

II. WHAT IS A SMART CARD?

A smart card is a small, tamperproof computer. The smart card itself contains a CPU and some non-volatile storage. In most cards, some of the storage is tamperproof while the rest is accessible to any application that can talk to the card. This capability makes it possible for the card to keep some secrets, such as the private keys associated with any certificates it holds. The card itself actually performs its own cryptographic operations.

Although smart cards are often compared to hard drives, they're "secured drives with a brain"—they store and process information. Smart cards are storage devices with the core mechanics to facilitate communication with a reader or coupler. They have file-system configurations and the ability to be partitioned into public and private spaces that can be made available or locked. They also have segregated areas for protected information, such as certificates, e-purses, and entire operating systems. In addition to traditional data storage states, such as read-only and read/write, some vendors are working with sub states best described as "add only" and "update only."

Smart cards currently come in two forms, contact and contactless.

Contact cards require a reader to facilitate the bidirectional connection. The card must be inserted into a device that touches the contact points on the card, which facilitate communication with the card's chip. Contact cards come in 3-volt and 5-volt models, as do current desktop CPUs. Contact card readers are commonly built into company or vendor-owned buildings and assets, cellular phones, handheld devices, stand-alone devices that connect to a computer desktop's serial or Universal Serial Bus (USB) port, laptop card slots, and keyboards.

Contactless cards use proximity couplers to get information to and from the card's chip. An antenna is wound around the circumference of the card and activated when the card is radiated in a specific distance from the coupler. The configuration of the card's antenna and the coupler facilitate connected states from a couple of centimeters to a couple of feet. The bidirectional transmission is encoded and can be encrypted by using a combination of a card vendor's hard-coded chip algorithms; randomly generated session numbers; and the card holder's certificate, secret key, or personal identification number (PIN). The sophistication of the connection can facilitate separate and discrete connections with multiple cards should they be within range of the coupler. Because contactless cards don't require physical contact with a reader, the usability range is expanded tremendously.

International standards govern the physical characteristics of smart cards. For example, the size of a card is covered by International Organization for Standardization (ISO) 7810. ISO 7816 and subsequent standards cover manufacturing parameters, physical and electrical characteristics, location of the contact points, communication protocols, data storage, and more. Data layout and format, however, can vary from vendor to vendor.

In addition to physical and manufacturing standards, an increasing number of standards exist for specific vendor applications. Credit card vendors, cellular phone vendors, Unites States and European banks, credit agencies, and debit agencies are examples of organizations that are tailoring smart card applications and procedures geared exclusively to the services they offer and the companies with which they do business.

The Microsoft Windows for Smart Cards operating system is a component-based architecture that supports multiple card chips and platforms. It's extensible and supported by a growing number of card manufacturers and vendors. Developers can integrate the application programming interfaces (APIs) and the associated toolkit into environments that are already familiar to them. You can obtain cards that are compliant with Windows for Smart Cards from a variety of sources. You can develop smart card applications by using systems such as Microsoft Visual Basic and Microsoft Visual C++. Internally, Microsoft is working with Windows for Smart Cards–compliant third-party vendors to provide enterprise management tools that are compatible with Microsoft Windows 2000 and later operating systems. These will provide additional administrative features, such as the ability to remotely reset PINs.

A number of vendors are providing support and other standards for Windows for Smart Cards. Sun Microsystems has published and currently maintains specifications for both Windows for Smart Cards and a "Java Card." Gemplus and Schlumberger also support Windows for Smart Cards, in addition to their own card operating system, the "Java Card" specification.

III. WHY A SMART CARD?

Smart cards are a key component of the public key infrastructure (PKI) that Microsoft is integrating into the Windows platform because smart cards enhance software-only solutions, such as client authentication, logon, and secure email. Smart cards are a point of convergence for public key certificates and associated keys because they:

- Provide tamper-resistant storage for protecting private keys and other forms of personal information
- Isolate security-critical computations, involving authentication, digital signatures, and key exchange from other parts of the system that don't have a need to know
- Enable portability of credentials and other private information between computers at work, at home, or on the road

The smart card has become an integral part of the Windows platform because smart cards provide new and desirable features as revolutionary to the computer industry as the introduction of the mouse or CD-ROM

Introducing Windows for Smart Cards

One of the newest members of the Windows operating system family, Windows for Smart Cards extends the benefits of the Windows environment to the smart card industry.

A Windows Powered Smart Card is a microcomputer without a graphical user interface (GUI). According to Gemplus, a leading smart card manufacturer, companies have reduced their technical support calls by 40 percent by implementing smart cards that perform automatic authentication, which previously was an error-prone manual process. Microsoft is working closely with smart card industry leaders such as Gemplus to develop its smart card technology to the highest performance and security standards in the enterprise. At the same time, Microsoft is integrating smart card technology with Windows-based architectures to facilitate ease of application development.

At a price of approximately $20 per card reader and a maximum of $5 per card, Windows Powered Smart Cards are an inexpensive way to strengthen your corporate security. Even when you implement the cards only for security reasons, your business still benefits from the multitude of other functions that Smart Cards facilitate. These services include payment functionality and storage of loyalty information, medical and citizen information, and personal contacts.

The Windows Powered Smart Card can enhance your existing corporate network; there's no need to replace the existing system infrastructure. Windows for Smart Cards works with all Windows releases since Windows 95.

You can customize Windows Powered Smart Cards for each user, and program the cards with multiple keys. The cards can be used to log on to a PC or to one or more networks and to perform remote logons. By storing all of a user's authentication information, one Windows Powered Smart Card can provide a user with admittance to all of their accounts—on the corporate network, within Internet chat rooms, or within financial institutions.

Therefore, Windows for Smart Cards used with one or more of the Microsoft Windows operating systems can enhance protection, improve productivity, increase profit, and facilitate promotion.

Enhanced Protection

Corporate computers generally are configured to require a form of authentication for logon purposes. Password authentication, the most widely used logon security mechanism, is only as infallible as its users. Users often share their personal passwords with friends and spouses. Even the most reliable user might write a password on a slip of paper where another user could discover it later. If a user doesn't safeguard a password, the network might be subject to concurrent usage of a user account or worse, be unprotected against malicious break-ins.

Only one person at a time can use a Windows Powered Smart Card, which makes concurrent account usage impossible. Because the card is required to access the network, users are inclined to carry the card with them wherever they go, thus preventing malicious break-ins. Windows for Smart Cards supports multiple authentication mechanisms, such as PIN, fingerprint, or retina recognition. Your company can determine the method or methods that work best for you.

If the card is lost, no one else can use it to access the network because only the owner knows the PIN or has the fingerprint or retina to match the authentication account. Information and account balances aren't lost if the card is lost because a user's information is replicated on each card partner's server. When a replacement card is activated and inserted into the card partner's network, the information is transferred to the new card.

Like a bank or credit card, if a Windows Powered Smart Card is lost or stolen, an 800 number can be used to turn off the card and activate the issuance of a new card. Unlike a bank or credit card, however, a Windows Powered Smart Card can be produced at a branch office for quicker turnaround. By using the most secure crypto-algorithms, such as RSA, DES, 3DES, AES, and SHA, and by being built on the most reliable chips, Windows Powered Smart Cards are virtually inviolable.

Improved Productivity

Windows for Smart Cards ensures a consistent experience for application developers and end users. Application developers can use development and debugging tools with which they're already proficient, such as Microsoft Visual Studio, to create applications for Windows Powered Smart Cards. Additionally, developers save time by using the Microsoft Windows Smart Card Toolkit to write applications. Unlike tools that differ from vendor to vendor, Windows for Smart Cards is a logical extension of the Windows operating systems and provides a consistent development and runtime environment. By using the Windows Smart Cards Toolkit with the Windows operating systems, developers can write and debug many diverse applications in the same amount of time it would have taken to port one application to many diverse operating environments.

You can use Windows Powered Smart Cards with the Windows operating systems to store personal contact information. By using the cards as a companion to the Microsoft Outlook messaging and collaboration client, you can transfer the names, email addresses, and phone numbers of business associates from a PC or network to the card. You can slip the card into your pocket or wallet; then, miles and time zones away, you can insert it into another computer running a Windows operating system. Instantly, your Outlook information is accessible.

Windows Powered Smart Cards can be used to store medical information and citizen accounts. Pharmacies can check a patient's card to verify that the patient isn't taking medication that might interact negatively with a new prescription. By using Windows Powered Smart Cards, a doctor's office can bill insurance companies at the time of treatment, eliminating copious paperwork and speeding the payment of charges. Furthermore, Windows Powered Smart Cards also can be used to help distribute food stamps, store traffic violations, and verify a consumer's age for tobacco and alcohol purchases. Smart Card acts as the identity key.

Increased Profit

With the adoption of e-commerce by the masses, fraud activity has increased dramatically. Stolen credit card numbers are used to purchase goods and services on the Internet, where signatures aren't required to prove identity. Underage users can access information and entertainment that are intended for more mature audiences. With Windows for Smart Cards, a Web site administrator can ascertain the identity of a user signing in to a chat room to ensure the safety of patrons. In addition, administrators of Web sites that contain adult content can ensure that only the intended audience views the material.

Internet merchants can implement Windows Powered Smart Cards to obtain a digital signature when a customer purchases goods and services. Such a digital signature would protect financial institutions as well, ensuring that only a card's owner can make purchases with the card. Windows Powered Smart Cards can be used in lieu of a bank or credit card in traditional purchasing scenarios as well. By writing a financial application and storing it on the card, a vendor can determine the payment method. Financial institutions can write applications for Windows Powered Smart Cards that store a prepaid value, deducting from it as purchases are made. Alternatively, developers can write applications for Windows Powered Smart Cards with the same Windows-based APIs they already use to interact with a server-side automatic billing program.

Richer Advertising

You can use Windows Powered Smart Cards much like a credit card to advertise your business and your corporate partners. You can also store loyalty information, such as airline miles and past purchase amounts, directly on the card. Or you can issue Windows Powered Smart Cards to your customers and sell advertising space on them.

Unlike a credit card, however, Windows Powered Smart Cards are read/writable. When your company's strategic alliances change, you don't need to manufacture more cards; instead, you can change the advertisements and loyalty information on the cards you've already issued.

REFERENCES

1. *www.google.com*
2. *www.Wikipedia.com*
3. *http://www.pcscworkgroup.com.*
4. *http://www.microsoft.com/technet/itsolutions/msf/default.mspx*
5. *http://www.microsoft.com/whdc/whql/resources/HCTsetup.mspx.*
6. *http://www.microsoft.com/whdc/archive/wdm.mspx.*
7. *http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/deploy/dgch_pki_odbg.mspx*
8. *http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/featfunc/2000pk.mspx*
9. *http://www.microsoft.com/technet/security/guidance/identitymanagement/smrtcdcb/default.mspx*